



**Estado do Ceará  
Poder Judiciário  
Tribunal de Justiça  
Comitê Gestor de Segurança da Informação  
Anexo I**

**PJSETIN2015004 – Implantação do Programa de Segurança Corporativa da Informação no âmbito do Poder Judiciário do Estado do Ceará**

**01/NSI01/CGSI/TJCE – Norma de Contas e Senhas para Usuários e Administradores**



## Sumário

1 Objetivo.....	3
2 Abrangência.....	3
3 Termos e Definições.....	3
4 Diretrizes.....	3
5 Competências e Responsabilidades.....	5
6 Penalidades.....	6
7 Vigência.....	7



## 1 Objetivo

1.1 Definir as diretrizes orientativas para os usuários em relação à utilização de Contas e Senhas bem como relacionadas à utilização de Contas de privilégio de administrador de rede, sistemas, serviços no âmbito do Poder Judiciário do Estado do Ceará.

## 2 Abrangência

2.1 Esta norma abrange todos os usuários que possuem ou são responsáveis por uma conta, bem como qualquer forma de acesso com privilégios de “administrador” de rede, **sistemas de informações, equipamentos locais, serviços e banco de dados** no ambiente de Tecnologia da Informação do Poder Judiciário do Estado do Ceará.

## 3 Termos e Definições

3.1 Usuário: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, conveniados, consultores, estagiários, e demais pessoas que se encontrem a serviço do Poder Judiciário do Estado do Ceará, utilizando em caráter temporário os recursos tecnológicos deste Poder.

3.2 Conta de Acesso: código de acesso atribuído a cada usuário. A cada código de acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos computacionais disponíveis.

3.3 Administrador de rede, sistemas, serviços: usuários que possuem contas que permitem acesso total e irrestrito a quaisquer recursos da rede, sistema ou serviço em que estão configuradas.

## 4 Diretrizes

4.1 Aplicadas a todos os usuários em todos os níveis de privilégios:

4.1.1 Toda conta de usuário precisa possuir senha e deve seguir os padrões estabelecidos nesta Norma;

4.1.2 Todas as senhas de acesso a rede, sistemas e serviços diversos do Poder Judiciário do Estado do Ceará deverão ser trocadas a cada 45 (quarenta e cinco) dias;

4.1.3 As contas de rede serão bloqueadas depois de 5 (cinco) tentativas inválidas de entrada. Para desbloquear o usuário deverá entrar em contato com a Central de



Atendimento de Tecnologia da Informação (Cati);

4.1.4 Na criação de uma nova conta de rede, o usuário receberá uma senha temporária, que corresponde ao nº do CPF, a qual deverá ser trocada no primeiro acesso;

4.1.5 As contas de rede que ficarem inativas por mais de 90 (noventa) dias corridos serão bloqueadas;

4.1.6 Toda conta possuirá um usuário e uma senha vinculada;

4.1.7 O mau uso de uma conta de acesso por terceiros, será de responsabilidade do seu titular, sujeitando-o às penalidades cabíveis;

4.1.8 No caso de suspeita do comprometimento de uma senha, o usuário poderá redefinir sua senha e caso não consiga deverá entrar em contato com a Cati;

4.1.9 As seguintes orientações devem ser observadas em relação as senhas:

4.1.9.1 Utilizar caracteres alfa-numéricas. Ex: Ip25O4;

4.1.9.2 Utilizar caixa alta e baixa. Ex: IpSTma;

4.1.9.3 Utilizar caracteres especiais tipo #, @, \$,% , &, !, \*, ?, \_/, <,::,, {}, [], =, +;

4.1.9.4 Conter no mínimo 6 (seis) caracteres;

4.1.9.5 Não utilizar o nome do usuário para senha. Ex: usuário: maria, senha: maria;

4.1.9.6 Não utilizar seu nome ou combinações deste, nomes de familiares, datas de aniversário, número de telefone;

4.1.9.7 Não utilizar informações pessoais ou fáceis de serem obtidas; e

4.1.9.8 Não repetir os mesmos números e letras. Ex: 111111, aaabbb.

4.2 Aplicadas a todos os Administradores de Rede, Sistemas e serviços em todos os níveis de privilégios:

4.2.1 As seguintes orientações devem ser observadas em relação as senhas:

4.2.1.1 Não utilizar senhas genéricas para seus acessos;

4.2.1.2 A senha deverá conter no mínimo 10 (dez) caracteres. No caso dos ambientes que não suportarem o mínimo de 10 caracteres, deverá ser utilizados o limite



máximo que o ambiente permitir;

4.2.1.3 Não será permitido a utilização de usuários administradores genéricos. Todo e qualquer usuário que possui ou é responsável por uma conta ou qualquer forma de acesso com privilégios de “administrador” de sistemas de informações, equipamentos locais, serviços ou banco de dados será associado a uma matrícula ou CPF que o identifique de forma individual.

4.3 A Secretaria de Tecnologia da Informação (Setin) deverá garantir:

4.3.1 A manutenção de um histórico composto, pelo menos, das 5 (cinco) últimas senhas, de forma a impedir que o usuário reutilize-as para renovação;

4.4 O tempo de vida das senhas para administradores: de máquina local, de domínio, de servidores físicos e virtuais, de sistemas de informações, de serviços e de banco de dados deverá ser de 45 (quarenta e cinco) dias, devendo ser forçada a troca no primeiro login após esse período.

4.5 As senhas de sistemas de informações ou banco de dados utilizadas em ambiente de produção deverão ser exclusivas e diferentes daquelas utilizadas em outros ambientes (treinamento, teste, homologação).

## **5 Competências e Responsabilidades**

### **5.1 Dos Usuários/Colaboradores**

5.1.1 Comunicar ao setor competente da Setin ou a sua chefia imediata qualquer violação a esta Norma.

5.1.2 Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de sua senha, através dos quais possa efetuar operações designadas nos recursos computacionais que acessa, procedendo a:

5.1.2.1 Trocar a senha temporária no primeiro acesso;

5.1.2.2 Não registrar a senha em papel, em local visível, no computador ou na Internet;

5.1.2.3 Nunca utilizar o recurso de “salvar senha” ou semelhantes em aplicações como navegadores, correio eletrônico, entre outras;

5.1.2.4 Trocar a senha quando houver indícios de haver sido comprometida e



comunicar o incidente a Setin através da Cati;

5.1.2.5 Não revelar senhas pelo telefone, e-mail ou por qualquer outro meio para qualquer pessoa, independente de hierarquia. O acesso à conta, e seus recursos atribuídos, é de responsabilidade pessoal e intransferível do titular.

## **5.2 Dos Custodiantes da Informação**

### **5.2.1 Da Área de Tecnologia da Informação**

5.2.1.1 Adotar mecanismos para bloquear a senha após 5 (cinco) tentativas inválidas.

5.2.1.2 Adotar mecanismos para não aceitar senha com menos de 6 (seis) caracteres.

5.2.1.3 Adotar mecanismos para garantir que as senhas expirem a cada 45 (quarenta e cinco dias).

5.2.1.4 Adotar mecanismos para forçar o usuário a trocar a senha no primeiro acesso.

5.2.1.5 Conscientizar os usuários na criação de senhas e a sua importância na segurança da informação.

### **5.2.2 Do Serviço de Segurança da Informação**

5.2.2.1 Promover divulgação das regras presentes nesta norma, acompanhar as auditorias dos sistemas e reportar ao Comitê Gestor de Segurança da Informação (CGSI) as ameaças à Política de Segurança da Informação.

### **5.2.3 Do Comitê Gestor de Segurança da Informação**

5.2.3.1 O comitê será acionado quando a área de Segurança da Informação julgar pertinente.

## **5.3 Do Monitoramento e da Auditoria do Ambiente**

5.3.1 Quando solicitada auditoria, a respectiva área de tecnologia da informação deverá prover as informações verificando a adoção das regras contidas nesta Norma.

## **6 Penalidades**



6.1 Uma vez que o usuário é responsável por qualquer atividade a partir de sua conta de rede ou sistemas, o mesmo responderá por qualquer ação legal apresentada ao Poder Judiciário do Estado do Ceará que envolva a suas contas.

6.2 No caso de evidências de uso irregular das contas de rede ou sistemas, o usuário terá seu acesso bloqueado para averiguação.

6.3 O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato e à diretoria correspondente.

6.4 O acesso somente será restabelecido mediante solicitação da chefia imediata, informando que tomou conhecimento da violação das normas de segurança.

6.5 Nos casos em que ficar evidente que o usuário permitiu ou facilitou, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública, o Comitê Gestor de Segurança da Informação será informado e tomará as medidas que julgar necessárias.

6.6 As penalidades poderão incluir: bloqueio temporário, cancelamento dos acessos, processos administrativos, criminais e cíveis, além da aplicação das penalidades previstas em lei.

## **7 Vigência**

7.1 Esta Norma entra em vigor na data de sua publicação.